[translation]

(19) KOREAN INTELLECTUAL PROPERTY OFFICE (KR)

(12) KOREAN PATENT LAID-OPEN PUBLICATION (A)

(51) Int. Cl.[6]
G06K 9/00

(11) Laid-Open Publication No.: 2003-0052194
(43) Laid-Open Publication Date: June 26, 2003

(21) Application No.: 2001-0082100
(22) Filing Date: December 20, 2001

(71) Applicant: Electronics and Telecommunications Research Institute

(72) Inventors: Jong-Mo Seong
Dong-Man Jang

(54) Title: A SYSTEM FOR USER AUTHENTIFICATION USING BIOMETRIC INFORMATION, A METHOD FOR REGISTERING A CERTIFICATE AND A METHOD FOR AUTHENTICATING USER IN THE SYSTEM.

ABSTRACT

The present invention relates to a system for authenticating user using biometric information such as a fingerprint, voice, retina, iris and the like, a method for registering a certificate to said authentication system and a method for authenticating a user.

The system for authenticating a user comprises: a plurality of biometric recognition systems generating a standard pattern by collecting biometric information from a user at the registration, requesting for the registration with the relevant information necessary for the authentication, receiving, inspecting and interpreting the certificate during the authentication, and performing the user authentication by using the standard pattern and the relevant information included in the certificate; a authentication authority storing and managing the authentication the information transmitted on the request for the registration from said plurality of biometric recognition systems in a database equipped inside, and searching and transmitting the certificate of the corresponding user upon a request for the certificate from said plurality of biometric recognition systems; and a network that enables to communicate by connecting said plurality of biometric recognition systems with the authentication authority, and thereby, a secure and convenient user authentication may be possible by resolving the inconvenience in registering the biometric information per biometric recognition system and the difficulty from storing a private key in a method for encrypting a public key.

Brief description of the drawings

Fig. 1 is a construction diagram of a user authentication system using biometric information according to the present invention.

Fig. 2 is a detailed construction diagram of a biometric recognition system of said Fig. 1.

Fig. 3 is a detailed construction diagram of the authentication authority of said Fig. 1.

Fig. 4 is a flow chart explaining the registration procedure generated in the biometric recognition system of the present invention.

Fig. 5 is a flow chart explaining the registration procedure generated in the authentication authority of the present invention.

Fig. 6 is a flow chart explaining the verification procedure generated in the biometric recognition system of the present invention.

Fig. 7 is a flow chart explaining the authentication procedure generated in the authentication authority of the present invention.

Fig. 8 is a format of the certificate including the biometric information used in the present invention.

Explanation of the reference numeral regarding the main part of the drawings

101~103: Biometric recognition system
104: Network

105: Authentication authority

Claims

1. A user authentication system using biometric information, comprising:

a plurality of biometric recognition systems generating a standard pattern by collecting biometric information from a user at the registration, requesting the registration with the relevant information necessary for the authentication, receiving, inspecting and interpreting the certificate at the authentication, and performing the user authentication by using the standard pattern and the relevant information included in the certificate;

a authentication authority storing and managing the authentication the information transmitted on the request for the registration from said plurality of biometric recognition systems in a database equipped inside and searching and transmitting the certificate of the corresponding user when there is a request for the certificate from said plurality of biometric recognition systems; and

a network that enables to communicate by connecting said plurality of biometric recognition systems with the authentication authority.

2. The user authentication system using the biometric information of Claim 1, wherein said authentication authority comprises:

a network interface device for performing a function of connecting with said network for communication with said plurality of biometric recognition systems;

a database for storing certificates;

a certificates generating block for generating the certificates by using a request for registering the certificates received from said biometric recognition system; and

a certificates management block for managing the certificates kept in said database through works such as searching, adding and deleting.

3. The user authentication system using the biometric information of Claim 1 or Claim 2, wherein each of said plurality of biometric recognition systems comprises:

a biometric information collecting device for collecting the biometric information of a human such as a fingerprint, voice, retina and iris;

a characteristic extracting block for extracting an unique characteristic pattern from the biometric information collected at said biometric information collecting device according to the designated processing information;

a pattern comparison block for performing a role for comparing a characteristic pattern provided from said characteristic extracting block with a standard pattern extracted from the certificate according to comparison information;

a deciding block for performing a function for outputting the authentication result by the user's decision of approval and rejection by using the decision information obtained from the certificate;

an authentication information for generating block for performing a function of making a message for transmitting to an authentication authority by combining the standard pattern regarding the user with process information, the comparison information and the decision information used when the standard pattern is made;

a network interface device for performing a connecting function with the network for communicating with the authentication authority; and

a certificates inspection and interpretation block for performing a function of extracting the standard pattern, the processing information and the decision information by checking and interpreting whether or not there is an error by inspecting the certificates

received through said network interface device from said authentication authority on the request for certificate.

4. A method for registering the certificate in the user authentication system using the biometric information, comprising:

a first step of receiving identifier, necessary information and biometric information by input from a user who wishes to register the biometric information at any one of a plurality of biometric recognition systems;

a second step of generating the standard pattern from said biometric information by using a pre-determined processing information;

a third step of generating a request message of registering the certificate by combining said generated standard pattern, said processing information, the comparison information and the decision information, and transmitting the request message of registering the certificate to the authentication authority;

a fourth step of generating the certificate according to a certificate format by using said registration request message received from the authentication authority;

a fifth step of checking whether or not there is a user by searching a database of said authentication authority, performing new registration or additional registration of the certificate according to the checking result, and transmitting to the checking result to the biometric recognition system requesting the registration; and

a sixth step of outputting the result in the biometric recognition system receiving said registration result to the user.

5. The method of registering the certificate in the user authentication system using the biometric information of Claim 4, wherein the work of said first step to third step is characterized by being performed in the biometric recognition system to register the certificate.

6. The method of registering the certificate in the user authentication system using the biometric information of Claim 4, wherein if there is a user in said fifth step, an additional registration is performed by adding the processing information, the pattern comparison information and the standard patter to the existing certificates.

7. A user authentication method of the user authentication system using the biometric information, comprising:

a first step of requesting the certificate to the authentication authority by receiving the information about a subject to be authenticated from the user in the biometric recognition system;

a second step of searching the certificate in the database on the request for the certificates of said first step and transmitting the corresponding certificate to said biometric recognition system;

a third step of performing inspection and interpretation on the certificates received in said biometric recognition system;

a fourth step of setting the processing information, the comparison information, the decision information and the standard pattern based on the result interpreted in said third step, and receiving the biometric information from the user by input;

a fifth step of extracting a test pattern using the processing information set in said fourth step and comparing said standard pattern and the test pattern by using said comparison information;

a sixth step of performing the decision procedure regarding the comparison result of

said fifth step by using said dscision information; and

a seventh step of approving or rejecting the user according to the decision result of said sixth step.

8. The user authcntication method of the user authentication system using the biometric information of Claim 7, wherein if there is no certificate requested by the user in said database or an error occurs in searching the certificate in said sccond step, the corresponding error mcssage is transmitted to said biometric recognition system.

Drawings

101: Biometric recognition system 1
102: Biometric recognition system 2
103: Biometric recognition system N
104: Network
105: Authentication authority
201: Biometric information collecting devicc
202: Characteristic extraction
203: Pattern comparison
204: Dccision
205: Generating verification information
206: Network interface dcvice
207: Certificates inspection and interpretation
301: Network interface device
302: Certificates generation
303: Certificates management
304: Database
400: Start
401: Receiving uscr information
402: Recciving biometric information
403: Loading proccss information
404: Extracting a standard pattern
405: Generating a registration request message
406: Requesting a rcgistration to verification authority
407: Receiving a rcgistration result
408: Outputting the result to user
490: End
500: Start
501: Receiving a registration request
502: Generating certificate
503: Scarching databasc
504: Does a uscr exist?
505: Rcgistering a new certificate
506: Transmitting a result message
507: Registcring an additional certificate
590: End
600: Start
601: Receiving user information
602: Requesting certificate to an Proccss information authority
603: Receiving a request result

604: Is it succeeded?
605: Inspecting and interpreting a certificate
606: Setting the process information
Setting the comparison information
Setting the decision information
607: Setting a standard pattern
608: Receiving a biometric information
609: Extracting characteristics
610: Pattern comparison
611: Decision
612: Is authentication succeeded?
613: Approval of user
614: Rejection of user
616: Outputting an error
690: End
700: Start
701: Receiving a certificate request
702: Extracting the user information and a biometric recognition type
703: Searching database
704: Is search succeeded?
705: Transmitting certificate
706: Transmitting an error
790: End
801: Certificate format version
802: Certificate serial number
803: Signature algorithm about an authentication authority
804: Authentication authority name
805: Term of validity
806: User name
807: Biometric recognition type
808: User biometric information
809: Process information
810: Comparison information
811: Decision information
812: Electronic signature

특2003-0052194

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
G06K 9/00

(11) 공개번호 특2003-0052194
(43) 공개일자 2003년06월26일

(21) 출원번호 10-2001-0082100
(22) 출원일자 2001년12월20일

(71) 출원인 한국전자통신연구원
대전 유성구 가정동 161번지

(72) 발명자 성중모
대전광역시유성구신성동123-10번지205호
장동만

(74) 대리인 손원, 함상준

심사청구 : 있음

(54) 생체정보를 이용한 사용자 인증 시스템, 상기 시스템에서인증서를 등록하는 방법 및 사용자 인증 방법

요약

본 발명은 지문, 음성, 망막, 홍채 등과 같은 생체정보를 이용한 사용자 인증 시스템, 상기 인증 시스템에서 인증서를 등록하는 방법 및 상기 시스템을 위한 사용자 인증 방법에 관한 것이다.

본 발명의 사용자 인증 시스템은, 등록시에는 사용자로부터 생체정보를 수집하여 기준패턴을 생성하고, 인증에 필요한 관련 정보와 함께 등록요청을 행하며, 인증시에는 인증서를 수신하여 이를 검사 및 해석하고, 인증서에 포함된 기준패턴과 관련정보를 이용하여 사용자 인증을 수행하는 복수의 생체인식 시스템; 상기 복수의 생체인식 시스템으로부터 등록요청을 통해 전송된 인증정보를 내부에 구비하고 있는 데이터베이스에 저장 및 관리하며, 상기 복수의 생체인식 시스템으로부터 인증서 요청이 있을 때, 해당 사용자에 대한 인증서를 검색하여 전달해주는 인증기관; 및, 상기 복수의 생체인식 시스템과 인증기관을 연결하여 통신이 가능하게 하는 네트워크를 포함함으로써, 생체인식 시스템마다 생체정보를 등록 해야 하는 불편함과 공개키 암호화 방식이 가지는 비밀키 저장의 어려움을 해결하면서 안전하고 편리한 사용자 인증을 가능하게 한다.

대표도

도1

색인어

생체정보, 사용자 인증, 인증서, 등록

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 생체정보를 이용한 사용자 인증 시스템의 구성도.

도 2는 상기 도 1의 생체인식 시스템을 상세하게 나타낸 구성도.

도 3은 상기 도 1의 인증기관을 상세하게 나타낸 구성도.

도 4는 본 발명의 생체인식 시스템에서 발생하는 등록 과정을 설명하는 순서도.

도 5는 본 발명의 인증기관에서 발생하는 등록 과정을 설명하는 순서도.

도 6은 본 발명의 생체인식 시스템에서 발생하는 인증 과정을 설명하는 순서도.

도 7은 본 발명의 인증기관에서 발생하는 인증 과정을 설명하는 순서도.

도 8은 본 발명에서 사용되는 생체정보를 포함하는 인증서의 포맷.

(도면의 주요 부분에 대한 부호의 설명)

101~103 : 생체인식 시스템 104 : 네트워크

105 : 인증기관

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 사용자 인증 시스템 및 이 시스템을 위한 등록 및 인증 방법에 관한 것으로서, 더욱 상세하게는 지문, 음성, 망막 등과 같은 생체정보를 이용한 사용자 인증 시스템, 상기 시스템에서 인증서를 등록하는 방법 및 상기 시스템을 위한 사용자 인증 방법에 관한 것이다.

기존의 생체인식을 이용한 사용자 인증은 지문, 음성, 망막과 같이 사람이 가지는 고유한 특징을 이용하여 사람을 인증하는 방법으로서, 접근 및 휴대가 용이하다는 장점이 있는 반면, 인증이 필요한 응용마다 매번 등록과정을 거쳐야 하는 단점이 있다. 사용자 인증에 관한 다른 분야의 기술로는, 공개키 암호화 방식의 인증서를 이용하는 방법이 있다. 이 방법은 인증기관을 이용하므로 일반적인 생체인식이 가지는 단점을 해결할 수 있지만, 이 방법의 특징상 사람이 기억하기 어려운 길이를 갖는 비밀키를 저장해야 하는 어려움이 있다. 이를 해결하기 위해서, 휴대가 가능한 스마트 카드에 비밀키를 저장하거나 PC(personal computer)의 저장장치에 비밀번호를 이용해서 저장하는 방법 등이 사용되고 있다. 그러나 전자의 경우, 분실의 위험이 따를 뿐만 아니라, 스마트카드 리더(reader)가 필요하다는 단점이 있으며, 후자의 경우에는 비밀번호 유출에 따른 도용의 위험이 따른다.

한편, 생체정보를 이용한 기술로서, 사용자의 지문에 기초하여 발생된 비밀키에 대응하는 공개키를 인증기관에 수신하여 디지털 증명서에 공개키를 포함시키도록 한 '생체 측정 데이터를 이용한 암호키 발생 방법(이하, '선행특허 1'이라 함)'이 대한민국 특허공개 제2001-52105호(공개일 : 2001년 6월 25일)에 공개된 바 있다. 상기 선행특허 1은 생체정보로부터 암호키를 발생시키는 것을 목적으로 하고 있으며, 생체정보를 인증서에 포함시켜 사용자를 인증하는 것에 관해서는 전혀 설명하고 있지 않다.

생체정보를 이용한 다른 선행 기술로서, 사용자의 생체정보를 입력받아 생체인식 데이터를 생성하고, 미리 등록된 생체인식 데이터와 비교하여 컴퓨터의 부팅 제어를 수행하는 '생체인식 장치를 이용한 컴퓨터 부팅 제어장치(이하, '선행특허 2'라 함)'가 대한민국 특허공개 제2001-11347호(공개일 : 2001년 2월 15일)에 공개된 바 있다. 상기 선행특허 2는 여러가지 생체정보를 이용하여 컴퓨터 부팅을 위한 인증을 목적으로 하고 있으나, 위 선행특허 1과 마찬가지로, 생체정보를 인증서에 포함시켜 사용자를 인증하는 것에 관해서는 전혀 설명하고 있지 않다.

생체정보를 이용한 또다른 선행 기술로서, 생체정보를 입력받아 디지털 처리를 통해 인식 수단을 미리 저장된 등록 데이터에서 탐색하여 출입 허가된 사람인지 판단하는 '생체인식에 의한 출입 통제방법 및 그 장치(이하, '선행특허 3'이라 함)'가 대한민국 특허공개 제2001-19345호(공개일 : 2001년 3월 15일)에 공개된 바 있다. 상기 선행특허 2는 생체정보를 이용하여 출입을 통제하는데 그 목적이 있으나, 위 선행특허들과 마찬가지로, 생체정보를 인증서에 포함시켜 사용자를 인증하는 것에 관해서는 전혀 설명하고 있지 않다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 바와 같은 기술적 배경 하에 이루어진 것으로서, 생체인식이 응용기기에 따라 별도의 등록과정을 거쳐야 한다는 문제와, 공개키 암호화 방식의 인증서를 이용한 인증방법이 가지는 비밀키 저장의 어려움을 해결하여 편리하고 안전한 사용자 인증 시스템, 상기 시스템에서 인증서를 등록하는 방법 및 상기 시스템을 위한 사용자 인증 방법을 제공하는데 목적이 있다.

발명의 구성 및 작용

상기한 목적을 달성하기 위한 본 발명의 사용자 인증 시스템은,

등록시에는 사용자로부터 생체정보를 수집하여 기준패턴을 생성하고, 인증에 필요한 관련 정보와 함께 등록요청을 행하며, 인증시에는 인증서를 수신하여 이를 검사 및 해석하고, 인증서에 포함된 기준패턴과 관련정보를 이용하여 사용자 인증을 수행하는 복수의 생체인식 시스템; 상기 복수의 생체인식 시스템으로부터 등록요청을 통해 전송된 인증정보를 내부에 구비하고 있는 데이터베이스에 저장 및 관리하며, 상기 복수의 생체인식 시스템으로부터 인증서 요청이 있을 때, 해당 사용자에 대한 인증서를 검색하여 전달해주는 인증기관; 및, 상기 복수의 생체인식 시스템과 인증기관을 연결하여 통신이 가능하게 하는 네트워크를 포함하는 것을 특징으로 한다.

또한, 상기한 목적을 달성하기 위한 본 발명의 인증서를 등록하는 방법은,

복수의 생체인식 시스템 중 어느 하나에서 생체정보를 등록하기를 원하는 사용자로부터 아이디, 필요 정보 및 생체정보를 입력받는 제1단계; 미리 설정된 처리정보를 이용하여 상기 생체정보로부터 기준패턴을 생성하는 제2단계; 상기 생성된 기준패턴, 상기 처리정보, 비교정보 및 판단정보를 취합하여 인증서 등록요청 메시지를 생성하여 인증기관에 전송하는 제3단계; 인증기관에서 상기 수신된 등록요청 메시지를 이용하여 인증서 포맷에 맞게 인증서를 생성하는 제4단계; 상기 인증기관의 데이터베이스를 검색하여 사용자 존재여부를 확인하고, 그 결과에 따라 인증서 신규 등록 또는 추가 등록을 수행한 후, 그 결과를 등록요청한 생체인식 시스템에 전송하는 제5단계; 및, 상기 등록 결과를 수신한 생체인식 시스템에서 그 결과를 사용자에게 출력하는 제6단계를 포함하는 것을 특징으로 한다.

또한, 상기한 목적을 달성하기 위한 본 발명의 사용자 인증 방법은,

생체인식 시스템에서 사용자로부터 인증하려는 대상에 대한 정보를 수신하여 인증기관에 인증서를 요청하는 제1단계; 상기 제1단계의 인증서 요청에 따라 데이터베이스에서 인증서를 검색하여 해당하는 인증서를

상기 생체인식 시스템에 전송하는 제2단계; 상기 생체인식 시스템에서 수신된 인증서에 대한 검사 및 해석을 수행하는 제3단계; 상기 제3단계에서 해석된 결과를 바탕으로 처리정보, 비교정보, 판단정보 및 기준패턴을 설정하며, 사용자로부터 생체정보를 입력받는 제4단계; 상기 제4단계에서 설정된 처리정보를 이용하여 테스트패턴을 추출하고, 상기 비교정보를 이용하여 상기 기준패턴과 테스트패턴을 비교하는 제5단계; 상기 판단정보를 이용하여 상기 제5단계의 비교결과에 대한 판단과정을 수행하는 제6단계; 및, 상기 제6단계의 판단 결과에 따라 사용자를 승인 또는 거부하는 제7단계를 포함하는 것을 특징으로 한다.

이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세하게 설명한다.

도 1에는 본 발명에 따른 생체정보를 이용한 사용자 인증 시스템의 구성이 도시되어 있다.

상기 도 1에 도시되어 있듯이, N개의 생체인식 시스템(101, 102, 103)과 인증기관(105)은 네트워크(104)로 연결되어 있다.

상기 각 생체인식 시스템(101, 102, 103)은 사용자로부터 생체정보를 수집하여 기준패턴을 생성한 다음, 인증에 필요한 관련 정보와 함께 인증기관(105)에 등록을 행한다. 또한, 상기 각 생체인식 시스템(101, 102, 103)은 상기 인증기관(105)으로부터 수신된 인증서를 검사 및 해석하고, 인증서에 포함된 기준패턴과 관련정보를 이용하여 사용자 인증을 수행한다.

상기 인증기관(105)은 복수개의 생체인식 시스템(101, 102, 103)으로부터 사용자 등록요청을 통해 전송된 인증정보를 내부에 구비하고 있는 데이터베이스에 저장 및 관리한다. 또한, 상기 인증기관(105)은 상기 각 생체인식 시스템(101, 102, 103)으로부터 인증서 요청이 있을 때, 해당 사용자에 대한 인증서를 검색하여 전달해주는 기능을 수행한다.

도 2에는 상기 도 1에 도시된 생체인식 시스템 중 하나에 대한 상세한 구성이 도시되어 있다.

상기 도 2에 도시되어 있듯이, 생체인식 시스템은 생체정보 수집장치(201), 특징추출 블록(202), 패턴비교 블록(203), 판단 블록(204), 인증정보 생성 블록(205), 네트워크 인터페이스 장치(206) 및 인증서 검사 및 해석 블록(207)으로 구성된다.

상기 생체정보 수집장치(201)는 지문, 음성, 망막, 홍채와 같은 사람의 생체정보를 수집하는 장치로서, 스캐너(scanner), 마이크, 카메라 등이 사용될 수 있다.

상기 특징추출 블록(202)은 지정된 처리정보에 따라 상기 생체정보 수집장치(201)에 수집된 생체정보로부터 고유한 특징패턴을 추출한다. 여기서, 처리정보는 각 생체 특징에 따른 특징추출 알고리즘 및 그 알고리즘에 사용되는 변수들을 포함한다.

상기 패턴비교 블록(203)은 상기 특징추출 블록(202)으로부터 제공된 특징패턴과, 인증서로부터 추출된 기준패턴을 비교정보에 따라 비교하는 역할을 수행한다. 여기서, 비교정보는 각 생체특징에 따른 패턴매칭 알고리즘 및 그 알고리즘에 사용되는 변수를 포함한다.

상기 판단 블록(204)은 인증서로부터 얻어진 판단정보를 이용해서 사용자의 승인 및 거절 등의 판단을 통해 인증결과를 출력하는 기능을 수행한다. 여기서, 판단정보는 각 생체 특징에 따른 판단을 위한 임계값 등을 포함한다.

상기 인증정보 생성 블록(205)은 사용자에 대한 기준패턴과 그 기준패턴을 만들 때 사용된 처리정보 및 비교정보, 판단정보를 취합하여 인증기관에 전송하기 위한 메시지를 만드는 기능을 한다.

상기 네트워크 인터페이스 장치(206)는 도 1에 도시된 인증기관(105)과 통신을 하기 위한 네트워크와의 연결 기능을 수행한다.

상기 인증서 검사 및 해석 블록(207)은 인증서 요청을 통해 상기 인증기관(105)으로부터 네트워크 인터페이스 장치(206)를 통해 수신된 인증서를 검사하여 오류가 없는지 확인한 다음, 해석하여 기준패턴, 처리정보, 비교정보 및 판단정보를 추출하는 기능을 한다.

도 3에는 상기 도 1의 인증기관이 상세하게 도시되어 있다.

상기 도 3에 도시되어 있듯이, 본 발명의 인증기관은 네트워크 인터페이스 장치(301), 인증서 생성 블록(302), 인증서 관리 블록(303) 및 데이터베이스(304)로 구성된다.

상기 네트워크 인터페이스 장치(301)는 상기 도 1의 생체인식 시스템(101, 102, 103)과의 통신을 위해 네트워크와의 연결 기능을 수행한다.

상기 인증서 생성 블록(302)은 생체인식 시스템에서 수신된 인증서 등록 요청 메시지를 이용하여 데이터베이스(304)에 저장할 인증서를 생성하는 기능을 한다.

상기 인증서 관리 블록(303)은 데이터베이스(304)에 보관되어 있는 인증서를 검색, 추가 및 삭제 등의 작업을 통해 관리하는 기능을 한다. 상기 데이터베이스(304)는 인증서를 저장하기 위한 장치이다.

도 4에는 본 발명의 생체인식 시스템에서 발생하는 등록 과정을 설명하는 순서도가 도시되어 있다.

동작이 시작되면(400), 상기 각 생체인식 시스템(101, 102, 103)은 자신의 생체정보를 등록하기를 원하는 사용자로부터 자신의 고유한 아이디와 필요한 정보를 수신한다(401). 그리고, 생체정보 수집장치(201)를 통해서 사용자의 생체정보를 입력받는다(402). 이어서, 상기 각 생체인식 시스템(101, 102, 103)에 미리 설정된 처리정보를 로딩(loading)한 다음(403), 상기 특징추출 블록(202)을 통해서 기준패턴을 생성한다(404). 상기 단계(404)를 통해 생성된 기준패턴과 상기 단계(403)의 처리정보, 비교정보 및 판단정보를 모아서 인증서 등록요청 메시지를 생성한다(405). 상기 등록 요청 메시지는 네트워크 인터페이스 장치(206)를 통해 인증기관(105)으로 전송한다(406). 다음으로, 상기 인증기관(105)으로부터 등록결과를 응답으로서 수신하여(407), 사용자에게 그 결과를 출력한다(408).

도 5에는 본 발명의 인증기관에서 발생하는 등록 과정을 설명하는 순서도가 도시되어 있다.

동작이 시작되어(500), 상기 인증기관(105)이 등록요청 메시지를 수신하면(501), 해당 메시지를 이용하여 인증서 포맷에 맞게 인증서를 생성한다(502). 그리고, 사용자 정보를 이용하여 데이터베이스를 검색하여(503), 사용자에 대한 이전 기록이 있는지 확인한다(504). 만약 존재하지 않는다면, 신규로 인증서를 등록하고(505), 존재하면 기존 인증서에 처리정보, 패턴비교정보, 기준패턴 등을 추가하여 등록한다(507). 마지막으로, 그 결과를 등록 요청한 생체인식 시스템으로 전송한다(506).

도 6에는 본 발명의 생체인식 시스템에서 발생하는 인증 과정을 설명하는 순서도가 도시되어 있다.

동작이 시작되면(600), 사용자로부터 인증하려는 대상에 대한 정보를 수신한다(601). 생체인식 시스템은 인증기관에 인증대상 사용자 및 생체인증 타입(type)에 대한 인증서를 요청하고(602), 그 결과를 수신한다(603). 다음으로, 인증서를 성공적으로 수신했는지 여부를 확인하며(604), 만약 성공이라면, 인증서에 대한 검사 및 해석을 수행하고(605), 실패라면 오류메시지를 사용자에게 출력한다(615). 다음으로, 상기 단계(605)에서 인증서 해석을 통해 나오는 처리정보, 비교정보 및 판단정보와 기준패턴을 차례로 설정하고(606, 607), 사용자로부터 생체정보를 입력 받는다(608). 상기 단계(606)에서 설정된 처리정보를 이용해서 생체인식 시스템의 특징추출 블록에서 테스트패턴을 추출한다(609). 다음으로, 기준패턴과 테스트패턴을 비교하고(610), 판단정보를 이용해서 판단과정을 거친다(611). 그 결과가 성공인지 확인하여(612), 성공이면 사용자를 승인하고(613), 실패이면 사용자를 거부한다(614).

도 7에는 본 발명의 인증기관에서 발생하는 인증 과정을 설명하는 순서도가 도시되어 있다.

동작이 시작되면(700), 상기 생체인식 시스템으로부터 인증서 요청을 수신한다(701). 다음으로, 인증서 요청 메시지에 포함된 사용자 정보와 생체인식 타입을 이용해서 데이터베이스에서 인증서를 검색한다(702, 703). 검색결과를 확인하고(704), 성공이면 해당 인증서를 생체인식 시스템으로 전송하고(705), 데이터베이스에 요청한 사용자에 대한 인증서가 없거나, 검색 오류라면 해당 오류 메시지를 전송한다(706).

도 8은 본 발명에서 사용된 생체인증정보를 포함하는 인증서의 포맷을 나타낸 것이다. 이 인증서 포맷은 X.509 표준 인증서 양식에 기반을 둔 것이다. 인증서 포맷 버전(801)은 해당 인증서 포맷에 대한 버전을 나타내는 것이고, 인증서 일련 번호(802)는 인증기관이 부여하는 고유한 번호로 해당 인증기관이 생성한 다른 인증서와 구분하는데 사용된다. 인증기관에 대한 서명 알고리즘(803)은 인증기관이 인증서에 전자서명을 할 때 사용되는 알고리즘을 지정한다. 인증기관 이름(804)은 인증기관의 이름을 지정하는 필드이고, 유효기간(805)은 해당 인증서의 유효한 사용가능 기간을 지정한다. 사용자 이름(806)은 생체정보를 제공한 사용자의 고유한 이름을 가리킨다. 생체인식 타입(807)은 음성, 지문, 홍채 등의 사용된 생체정보의 종류를 의미하며, 사용자의 생체 기준패턴은 사용자 생체정보(808)에 저장되고, 특징추출에 사용되는 처리정보, 비교정보 및 판단정보는 처리정보 필드(809)와 비교정보 필드(810), 판단정보 필드(811)에 각각 지정된다. 마지막으로 상기의 모든 필드에 대한 인증기관의 전자서명(812)을 덧붙여서 인증서를 만든다.

발명의 효과

본 발명에 따른 사용자 인증 방법을 이용하면, 별도의 사용자 등록 없이 한 번의 생체정보 등록으로 여러 시스템에서 그 등록정보를 효과적으로 공유할 수 있고, 음성, 지문, 홍채 등 다양한 형태의 생체정보도 함께 수용할 수 있으며, 별도의 인증에 필요한 키를 저장하는 장치 없이 사용자 인증을 할 수 있다.

(57) 청구의 범위

청구항 1

등록시에는 사용자로부터 생체정보를 수집하여 기준패턴을 생성하고, 인증에 필요한 관련 정보와 함께 등록요청을 행하며, 인증시에는 인증서를 수신하여 이를 검사 및 해석하고, 인증서에 포함된 기준패턴과 관련정보를 이용하여 사용자 인증을 수행하는 복수의 생체인식 시스템;

상기 복수의 생체인식 시스템으로부터 등록요청을 통해 전송된 인증정보를 내부에 구비하고 있는 데이터베이스에 저장 및 관리하며, 상기 복수의 생체인식 시스템으로부터 인증서 요청이 있을 때, 해당 사용자에 대한 인증서를 검색하여 전달해주는 인증기관; 및

상기 복수의 생체인식 시스템과 인증기관을 연결하여 통신이 가능하게 하는 네트워크를 포함하는 것을 특징으로 하는 생체정보를 이용한 사용자 인증 시스템.

청구항 2

제1항에 있어서,

상기 인증기관은,

상기 복수의 생체인식 시스템과의 통신을 위해 상기 네트워크와의 연결 기능을 수행하는 네트워크 인터페이스 장치;

인증서를 저장하고 있는 데이터베이스;

상기 생체인식 시스템에서 수신된 인증서 등록요청을 이용하여 인증서를 생성하는 인증서 생성 블록; 및

상기 데이터베이스에 보관되어 있는 인증서를 검색, 추가 및 삭제와 같은 작업을 통해 관리하는 인증서 관리 블록으로 구성됨을 특징으로 하는 생체정보를 이용한 사용자 인증 시스템.

청구항 3

제1항 또는 제2항에 있어서,

상기 복수의 생체인식 시스템 각각은,

지문, 음성, 망막, 홍채와 같은 사람의 생체정보를 수집하는 생체정보 수집장치;

지정된 처리정보에 따라 상기 생체정보 수집장치에서 수집된 생체정보로부터 고유한 특징패턴을 추출하는 특징추출 블록;

상기 특징추출 블록으로부터 제공된 특징패턴과, 인증서로부터 추출된 기준패턴을 비교정보에 따라 비교하는 역할을 수행하는 패턴비교 블록;

인증서로부터 얻어진 판단정보를 이용해서 사용자의 승인 및 거절의 판단을 통해 인증결과를 출력하는 기능을 수행하는 판단 블록;

사용자에 대한 기준패턴과 그 기준패턴을 만들 때 사용된 처리정보 및 비교정보, 판단정보를 취합하여 인증기관에 전송하기 위한 메시지를 만드는 기능을 수행하는 인증정보 생성 블록;

인증기관과 통신하기 위해 네트워크와의 연결 기능을 수행하는 네트워크 인터페이스 장치; 및,

인증서 요청을 통해 상기 인증기관으로부터 상기 네트워크 인터페이스 장치를 통해 수신된 인증서를 검사하여 오류가 없는지 확인하고, 해석하여 기준패턴, 처리정보, 비교정보 및 판단정보를 추출하는 기능을 수행하는 인증서 검사 및 해석 블록으로 구성됨을 특징으로 하는 생체정보를 이용한 사용자 인증 시스템.

청구항 4

복수의 생체인식 시스템 중 어느 하나에서 생체정보를 등록하기를 원하는 사용자로부터 아이디, 필요 정보 및 생체정보를 입력받는 제1단계;

미리 설정된 처리정보를 이용하여 상기 생체정보로부터 기준패턴을 생성하는 제2단계;

상기 생성된 기준패턴, 상기 처리정보, 비교정보 및 판단정보를 취합하여 인증서 등록요청 메시지를 생성하여 인증기관에 전송하는 제3단계;

인증기관에서 상기 수신된 등록요청 메시지를 이용하여 인증서 포맷에 맞게 인증서를 생성하는 제4단계;

상기 인증기관의 데이터베이스를 검색하여 사용자 존재여부를 확인하고, 그 결과에 따라 인증서 신규 등록 또는 추가 등록을 수행한 후, 그 결과를 등록 요청한 생체인식 시스템에 전송하는 제5단계; 및,

상기 등록 결과를 수신한 생체인식 시스템에서 그 결과를 사용자에게 출력하는 제6단계를 포함하는 것을 특징으로 하는 생체정보를 이용한 사용자 인증 시스템에서 인증서를 등록하는 방법.

청구항 5

제4항에 있어서,

상기 제1단계 내지 제3단계의 작업은 인증서를 등록하고자 하는 생체인식 시스템에서 수행되는 것을 특징으로 하는 생체정보를 이용한 사용자 인증 시스템에서 인증서를 등록하는 방법.

청구항 6

제4항에 있어서,

상기 제5단계에서 사용자가 존재하면 기존 인증서에 처리정보, 패턴비교정보, 기준패턴을 추가함으로써 추가등록을 수행하는 것을 특징으로 하는 생체정보를 이용한 사용자 인증 시스템에서 인증서를 등록하는 방법.

청구항 7

생체인식 시스템에서 사용자로부터 인증하려는 대상에 대한 정보를 수신하여 인증기관에 인증서를 요청하는 제1단계;

상기 제1단계의 인증서 요청에 따라 데이터베이스에서 인증서를 검색하여 해당하는 인증서를 상기 생체인식 시스템에 전송하는 제2단계;

상기 생체인식 시스템에서 수신된 인증서에 대한 검사 및 해석을 수행하는 제3단계;

상기 제3단계에서 해석된 결과를 바탕으로 처리정보, 비교정보, 판단정보 및 기준패턴을 설정하며, 사용자로부터 생체정보를 입력받는 제4단계;

상기 제4단계에서 설정된 처리정보를 이용하여 테스트패턴을 추출하고, 상기 비교정보를 이용하여 상기 기준패턴과 테스트패턴을 비교하는 제5단계;

상기 판단정보를 이용하여 상기 제5단계의 비교결과에 대한 판단과정을 수행하는 제6단계; 및,

상기 제6단계의 판단 결과에 따라 사용자를 승인 또는 거부하는 제7단계를 포함하는 것을 특징으로 하는 생체정보를 이용한 사용자 인증 시스템의 사용자 인증 방법.

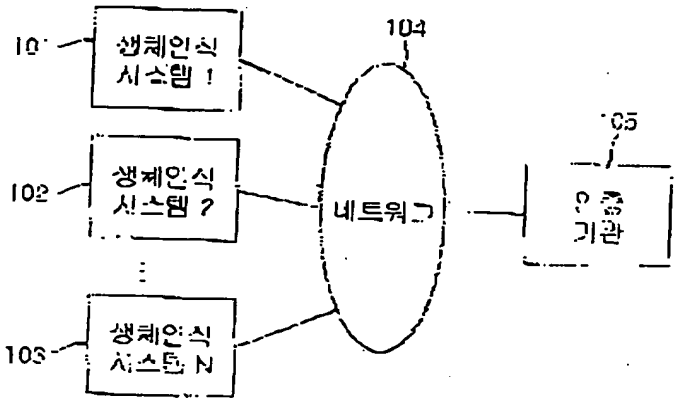
청구항 8

제7항에 있어서,

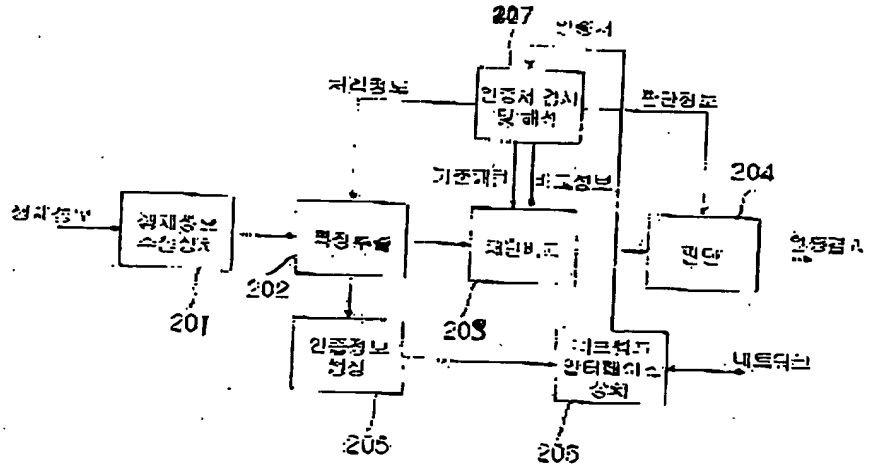
상기 제2단계에서 상기 데이터베이스에 사용자가 요청한 인증서가 없거나 검색 오류라면 해당 오류 메시지를 상기 생체인식 시스템에 전송하는 것을 특징으로 하는 생체정보를 이용한 사용자 인증 시스템의 사용자 인증 방법.

도면

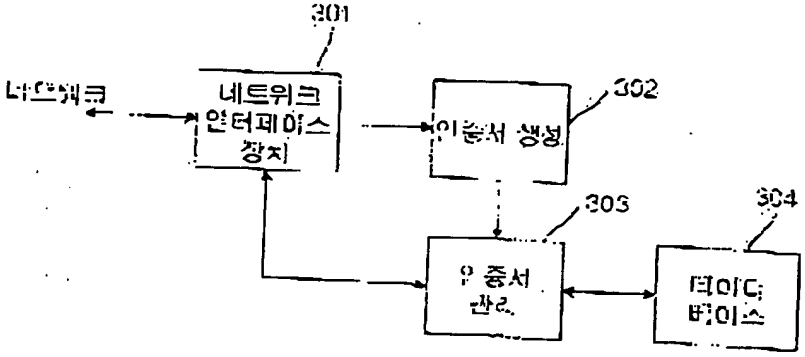
도면1



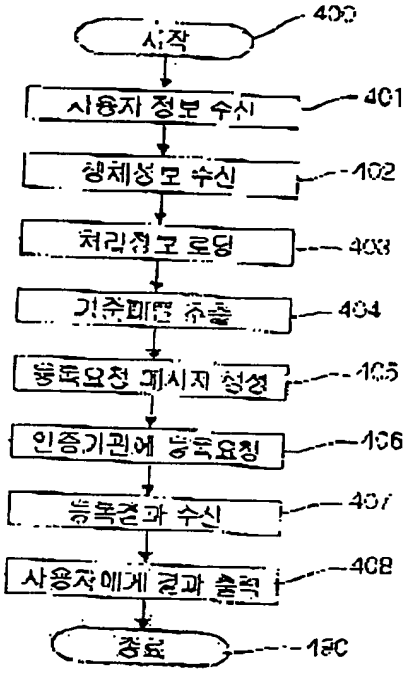
도면2



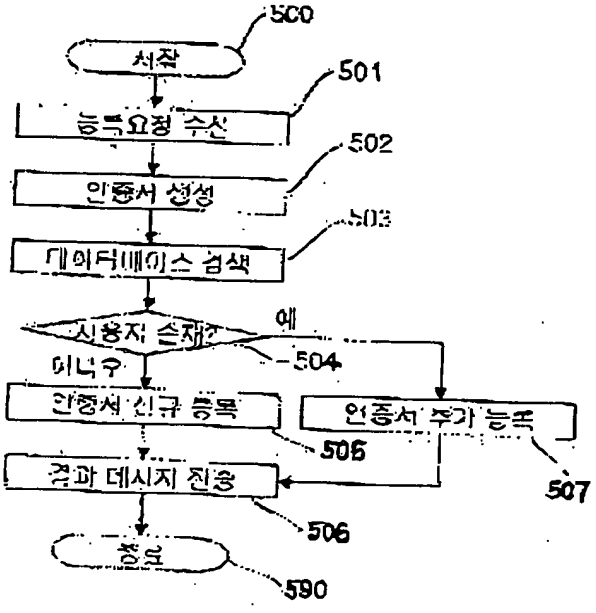
도면3



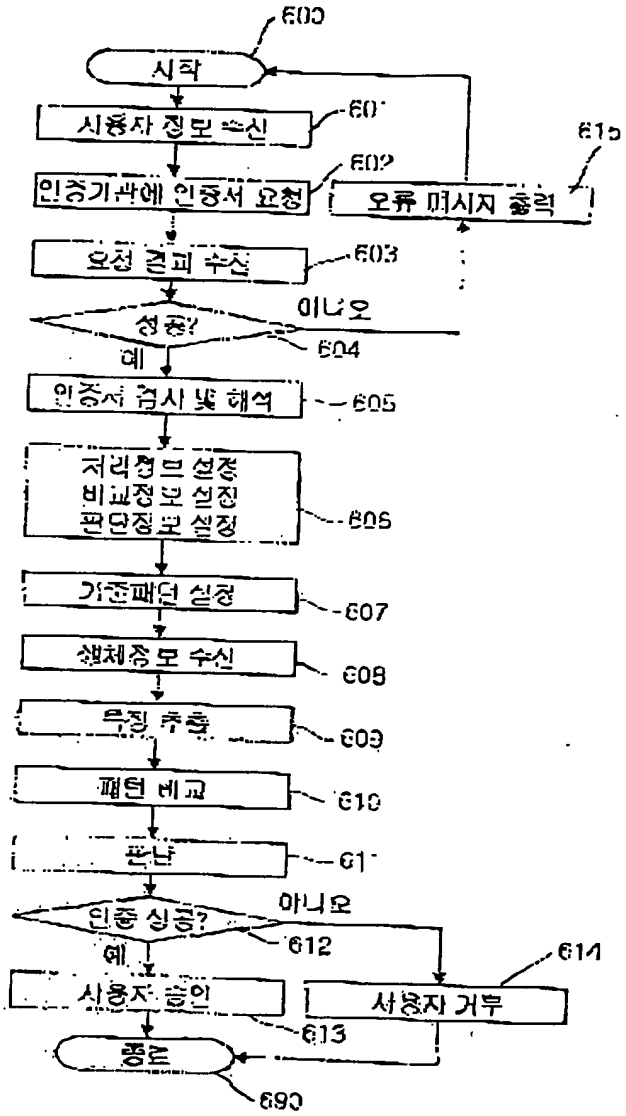
도면4


400
시작
401
사용자 정보 수신
402
생체정보 수신
403
처리정보 로딩
404
특징패턴 추출
405
등록요청 메시지 생성
406
인증기관에 등록요청
407
등록결과 수신
408
사용자에게 결과 출력
490
종료

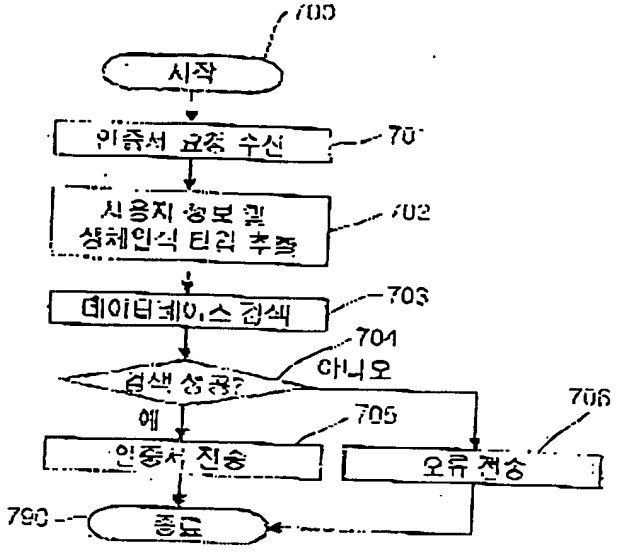
도면5


500
시작
501
등록요청 수신
502
인증서 생성
503
데이터베이스 검색
예
504
아니오
인증서 신규 등록
인증서 추가 등록
505
507
결과 메시지 전송
506
종료
590

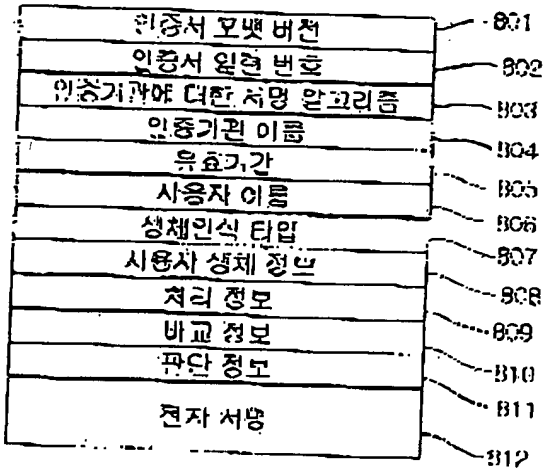
도면6


600
시작
601
사용자 정보 수신
602
인증기관에 인증서 요청
615
오류 메시지 출력
603
요청 결과 수신
아니오
성공?
604
예
605
인증서 검사 및 해석
606
저리정보 설정
비교정보 설정
판단정보 설정
607
기준패턴 설정
608
생체정보 수신
609
특징 추출
610
패턴 비교
611
판단
아니오
인증 성공?
612
예
614
사용자 거부
사용자 승인
613
종료
690

도면7


700
시작
인증서 요청 수신
701
사용자 정보 및 생체인식 타입 추출
702
데이터베이스 검색
703
704
검색 성공?
아니오
예
705
706
인증서 전송
오류 전송
790
종료

도면8


인증서 포맷 버전
801
인증서 일련 번호
802
인증기관에 대한 서명 알고리즘
803
인증기관 이름
804
유효기간
805
사용자 이름
806
생체인식 타입
807
사용자 생체 정보
808
처리 정보
809
비교 정보
810
판단 정보
811
전자 서명
812